

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) An information recording device comprising:
a memory unit containing data, including content data and a block permission
table defining memory-access control information, the for executing processing which
stores data to a memory unit having a data storage area ~~consisting of~~ comprising a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, ~~said information recording device comprising:~~
a processing unit for dividing content data into separate content data portions, for
storing each of the separate content data portions in a different sector within a first data
block of the data storage area, and for storing a security header corresponding to the
content data in a second data block of the data storage area;
a cryptosystem unit that selectively uses for performing sector level encryption by
using a different encryption key for each sector of the first data block from the first
sector to the M-th sector to execute encryption processing and the cryptosystem unit
executes encryption processing on the content data portion to be stored in each of the
sectors;
wherein the data includes a revocation list having revocation information
regarding revoked media or content and a block permission table for accessing a
permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the ~~revocation list and the~~
block permission table,

wherein the security header stored in the second data block includes each
encryption key used for each sector of the first data block.

Claims 2-4 (Cancelled).

5. (Currently Amended) An information recording device according to claim
1, wherein, in said cryptosystem unit, the encryption processing ~~for the first sector to the~~
~~M-th sector~~ is executed as single-DES encryption processing using different encryption
keys for ~~the sectors~~ each sector of the first data block.

6. (Currently Amended) An information recording device according to claim
1, wherein, in said cryptosystem unit, the encryption processing ~~for the first sector to the~~
~~M-th sector~~ is executed as triple-DES encryption processing using at ~~least~~ least two
different encryption keys for each ~~of the sectors~~ sector of the first data block.

Claim 7 (Cancelled).

8. (Currently Amended) An information playback device comprising:
a memory unit containing data, including encrypted content data and a block
permission table defining memory-access control information, the ~~for executing-~~
~~processing which reads data from a memory~~ unit having a data storage area ~~consisting-~~

~~of comprising~~ a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number ~~said information playback device comprising:~~

a processing unit for reading encrypted content data portions which together comprise encrypted content data, wherein each encrypted content data portion has been encrypted using a different encryption key and is read from a different sector within a first data block of the data storage area, and for reading a security header corresponding to the encrypted content data from a second data block of the storage area;

~~a cryptosystem unit which selectively uses~~ for performing sector level decryption by using a different decryption key for each sector of the first data block ~~from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on~~ the read encrypted content data portions stored in each of the sectors;

~~wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and~~

an integrity checking unit for checking the integrity of the ~~revocation list and the~~ block permission table,

wherein the security header read from the second data block includes each encryption key used to encrypt each encrypted content data portion read from the first data block.

Claims 9-11 (Cancelled).

12. (Currently Amended) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing ~~for the first sector to the M-th sector~~ is executed as single-DES decryption processing using different decryption keys ~~for the sectors~~ each sector of the first data block.

13. (Currently Amended) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing ~~for the first sector to the M-th sector~~ is executed as triple-DES decryption processing using at ~~least~~ least two different decryption keys for each ~~of the sectors~~ sector of the first data block.

Claims 14-16 (Cancelled).

17. (Currently Amended) An information recording method comprising the following steps performed by a control unit:

dividing content data into separate content data portions;

storing the separate content data portions and a block permission table defining memory-access control information, ~~for executing processing which stores data to a~~ memory medium having a data storage area ~~consisting of~~ comprising a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a

natural number, ~~said information recording method comprising:~~ each content data portion is stored in a different sector within a first data block of the data storage area and the security header is stored in a second data block of the data storage area;

~~encryption processing~~ encrypting, prior to storing, the content data to be stored in the sectors ~~portions~~ by performing sector level encryption using a different encryption key for each sector of the first data block in which a content data portion will be stored from the first sector to the M-th sector;

~~storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and~~

performing an integrity check of the ~~revocation list and the block permission table,~~

wherein the security header stored in the second data block includes each encryption key used to encrypt each content data portion stored in the sectors of the first data block.

Claims 18-20 (Canceled).

21. (Currently Amended) An information recording method according to claim 17, wherein ~~the encryption processing~~ encrypting is executed as single-DES encryption processing using different encryption keys ~~for the sectors~~ each sector of the first data block.

22. (Currently Amended) An information recording method according to claim 17, wherein ~~the encryption processing~~ encrypting is executed as triple-DES encryption processing using at least two different encryption keys for each ~~of the sectors~~ sector of the first data block.

Claim 23 (Cancelled).

24. (Currently Amended) An information playback method comprising the following steps performed by a control unit:
reading encrypted content data portions, which together comprise encrypted content data, a block permission table defining memory-access control information, and a security header ~~for executing processing which reads data~~ from a memory medium having a data storage area ~~consisting of~~ comprising a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, ~~said information playback method comprising:~~ each encrypted content data portion having been encrypted using a different encryption key and read from a different sector within a first data block of the data storage area, and the security header read from a second data block of the data storage area;

decrypting the content data portions stored in each of the sectors by ~~executing~~ performing sector level decryption processing by using a different decryption key for each sector ~~from the first sector to the M-th sector~~ of the first data block to execute decryption processing on the read encrypted content data portions;

~~storing data including a revocation list having revocation information regarding
revoked media or content and a block permission table for accessing a permission table
that describes memory access control information; and~~

~~performing an integrity check of the revocation list and the block permission
table,~~

wherein the security header read from the second data block includes each
encryption key used to encrypt each encrypted content data portion read from the first
data block.

Claims 25-27 (Cancelled).

28. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing is executed as single-DES decryption processing using different decryption keys for the sectors each sector of the first data block.

29. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing is executed as triple-DES decryption processing using at least two decryption keys for each of the sectors sector of the first data block.

Claim 30 (Cancelled).

31. (Currently Amended) A computer-readable medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising:

dividing content data into separate content data portions;

storing the separate content data portions, a block permission table, and a security header in a memory unit having a data storage area ~~consisting of~~ comprising a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, each content data portion being stored in a different sector within a first data block of the data storage area and the security header being stored in a second data block of the data storage area;

~~encryption processing~~ encrypting, prior to storing, the content data to be stored in the sectors portions by performing sector level encryption using a different encryption key for each sector of the first data block in which a content data portion will be stored from the first sector to the M-th sector;

~~storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and~~

checking the integrity of the revocation list and the block permission table,

wherein the security header stored in the second data block includes each encryption key used for each sector of the first data block.

32. (Currently Amended) A computer readable medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising:

reading encrypted content data portions, which together comprise encrypted content data, a block permission table defining memory-access control information, and a security header from a memory having a data storage area ~~consisting of~~ comprising a plurality of blocks, each of the blocks ~~consists of~~ comprising M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, each encrypted content data portion having been encrypted using a different encryption key and read from a different sector within a first data block of the data storage area, and the security header read from a second data block of the data storage area;

decrypting the content data portions stored in each of the sectors by ~~executing~~ performing sector level decryption processing by using a different decryption key for each sector ~~from the first sector to the M-th sector~~ of the first data block to execute decryption processing on the read encrypted content data portions;

~~storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and~~

checking the integrity of the ~~revocation list and the~~ block permission table,
wherein the security header read from the second data block includes each encryption key used to encrypt each encrypted content data portion read from the first data block.